IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF:

Naoto KINJO : GROUP ART UNIT:2623

SERIAL NO: 09/981,920 : EXAMINER: CHANG, JON CARLTON

FILED: October 19, 2001 :

FOR: METHOD OF PREVENTING FALSIFICATION OF IMAGE

CERTIFICATION OF TRANSLATION

HONORABLE COMMISSIONER OF PATENTS & TRADEMARKS
P.O. Box 1450
Alexandria, VA 22313-1450

SIR:

I, Teiichiro OGAWA, residing at c/o ION PATENT of HAYAKAWA-TONAKAI BLDG. 3F., 12-5, IWAMOTO-CHO 2-CHOME, CHIYODA-KU, TOKYO 101-0032 JAPAN declare:

(1) that I know well both the Japanese and English languages;

(2) that I translated the attached document identified as corresponding to Japanese Application No.2000-320229 filed in Japan on October 20, 2000 from Japanese to English;

(3) that the attached English translation is a true and correct translation of the document attached thereto to the best of my knowledge and belief; and

(4) that all statements made of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements are made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both under 18 USC 1001, and that such false statements may jeopardize the validity of the application or any patent issuing thereon.

Date: April 20, 2005

T. Ogawa

Teiichiro OGAWA

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: October 20, 2000

Application Number: Japanese Patent Application
No. 2000-320229

Applicant: Fuji Photo Film Co., Ltd.

September 10, 2001

Commissioner,
Patent Office
Kozo OIKAWA

Certificate No. 2001-308313

[TYPE OF THE DOCUMENT] APPLICATION FOR PATENT

[REFERENCE NUMBER] FF887740

[FILING DATE] October 20, 2000

[DESTINATION] Commissioner of the Patent Office

[INTERNATIONAL PATENT CLASSIFICATION] H04N 1/387

[TITLE OF THE INVENTION] METHOD OF PREVENTING FALSIFICATION OF PHOTOGRAPHED IMAGE

[NUMBER OF CLAIMS] 2

[INVENTOR]

[DOMICILE OR RESIDENCE] c/o Fuji Photo Film Co., Ltd., 798, Miyanodai, Kaisei-machi, Ashigara-kami-gun, Kanagawa

[NAME] Naoto KINJO

[APPLICANT FOR PATENT]

[IDENTIFICATION NO.] 000005201

[NAME] Fuji Photo Film Co., Ltd.

[AGENT]

[IDENTIFICATION NO.] 100080159

[PATENT ATTORNEY]

[NAME] Mochitoshi WATANABE

[TELEPHONE NO.] 3864-4498

[INDICATION OF CHARGE]

[DEPOSIT RECORD NO.] 006910

[AMOUNT OF PAYMENT] 21000 yen

[LIST OF ATTACHED DOCUMENT]

[TYPE OF DOCUMENT] Specification 1 set

[TYPE OF DOCUMENT] Drawing 1 set

[TYPE OF DOCUMENT] Abstract 1 set

[GENERAL POWER OF ATTORNEY NO.] 9800463

[REQUEST FOR PROOF] YES

[TYPE OF THE DOCUMENT] Specification

[TITLE OF THE INVENTION] METHOD OF PREVENTING FALSIFICATION OF PHOTOGRAPHED IMAGE

[CLAIMS]

[Claim 1]

A method of preventing falsification of a photographed image, comprising the steps of:

extracting an image characteristic amount by a specified algorithm from the photographed image in a camera;

recording identification information of the photographed image in the camera and said image characteristic amount into a database of an authentication institution which authenticates a status that there is no falsification in the photographed image;

extracting an image characteristic amount by said specified algorithm from an authentication object image whose authentication is requested in said authentication institution, and comparing said extracted image characteristic amount with the image characteristic amount recorded in said database, upon the authentication object image in said authentication institution; and

judging whether or not said authentication object image

Certificate No. 2001-308313

is falsified after being photographed, based on consistency between both the image characteristic amounts acquired from said comparison in order to prevent the falsification of the photographed image based on the judgment.

[Claim 2]

A method of preventing falsification of a photographed image, comprising the steps of:

sending authentication data from an authentication institution for authenticating a status that there is no falsification in the photographed image to a camera, as well as recording said authentication data and identification information of the photographed image of said camera into a database in said authentication institution;

attaching said authentication data to said photographed image or embedding said authentication data into said photographed image with said camera when photographing said photographed image;

extracting said authentication data from an authentication object image whose authentication has been requested in said authentication institution, and comparing said extracted authentication data with the authentication data recorded in said database, upon the authentication

Certificate No. 2001-308313

object image in said authentication institution; and

judging whether or not said authentication object image is falsified after being photographed, based on consistency between both the extracted authentication data acquired from said comparison in order to prevent the falsification of the photographed image based on the judgment.

[DETAILED DESCRIPTION OF THE INVENTION]

[0001]

[Technical Field of the Invention]

The present invention relates to a method of preventing falsification of a photographed image, which prevents digital image data from being falsified by authenticating a status that there is no falsification in the digital image data which is photographed using a digital still camera etc.

[0002]

[Prior Art]

The exposure systems in photography technologies using silver halide have conventionally performed printing through analog exposure such as plane exposure and direct exposure in general. Specifically, the exposure has been performed in such a manner that a developed negative film is disposed at a predetermined printing position, light from a white

light source such as halogen lamp is irradiated thereon, and then a transmitted image from the negative film is formed on a photographic paper.

[0003]

Contrary thereto, a printing apparatus using digital exposure, i.e., a digital photo printer has been recently put into practical use. In this digital photo printer, a pieces of image recorded on photographic films such as a negative film and a color reversal film are read out photoelectrically, and the read out image is converted into digital signals. Thereafter, image data for recording is acquired through various kinds of digital image processing, and then a photosensitive material is subjected to scanning exposure using recording light modulated according to the image data. Subsequently, the image (latent image) is recorded, thus completing a (finished) print.

[0004]

Such a digital photo printer regards the images as digital image data. Therefore, this digital photo printer is capable of processing not only an image in the photographic film but also an image photographed by a digital still camera and image data recorded as digital data

in various recording mediums such as a magnetic recording medium, which is a CD-R; a flexible disc and a removal hard disc such as Zip and Jaz; and an optomagnetic recording medium such as an MO disc, and outputting them as a print.

[0005]

Such digital data has advantages that connection and transmission of data to an information processing / information-communication equipment such as a personal computer are easy. However, the digital data has disadvantages that the data can be relatively falsified freely because of easy data handling. Therefore, it has been difficult to prevent data falsification and to authenticate data validity.

For example, there occurs damage claim management of automobile insurance or the like owing to a traffic accident or the like. When a photographic image photographed by a digital camera is used as a photographic evidence for damage assessment, it has become a matter of concern how to see through and prevent dishonesty by falsification of the photographic image or replacement with a fake photographic image (counterfeiting of a photograph).

[0006]

One proposal for overcoming the foregoing problem has been made in the technical report of the Section of Electronics, Information and Communication Engineers. It is the technical report titled "Function of Preventing and Detecting Falsification of Digital Photograph in Insurance Claim Management Group Work System" by Kazuharu TOYOKAWA, Norishige MORIMOTO, Satoko TONEGAWA, Kouichi KAMIJO, and Akio KOIDE, pp.1 to pp.8, IE 99 to 38, published in September, 1999. According to this report, when an adjuster photographs a damaged car using the digital camera mounting a memory card with a specified (particular) identification (hereinafter called as "ID") information and a certification key embedded therein, the digital camera automatically writes a photographed date and an authentication mark into a memory card. When the memory card is read out using a device driver of a computer for reading out the memory card, presence of the authentication mark guarantees a fact that the photograph is both an authentic photograph and not a modified photograph.

[0007]

In addition to the conventional delivery of the image data using the recording medium such as the memory card,

data transmission through communication lines is also carried out. In this case, there may be a possibility that the data is illegally falsified or replaced with fake data by a third person or a third party. Therefore, security protection in communication has become a matter of concern.

In order to overcome the foregoing problem, various methods of preventing data replacement on purpose and falsification have been heretofore examined, such as a method of encrypting and transmitting information that guarantees validity of data, a method employed for an electronic signature and a method employed for an electronic watermark technique in which invisible information is embedded into an image.

[0008]

[Problems to be Solved by the Invention]

However, data is transmitted from the camera via the memory card using a predetermined protocol in the proposal disclosed in the above-mentioned gazette. Therefore, a memory card having a specific hardware authentication function is required, and this is not thus suitable when it is to be used by unspecified number of users. Accordingly, realization of a system has been desired, such as being

capable of authenticating a status that an image is not falsified, without requiring any recording medium having a special function as above-mentioned.

Further, as mentioned above, various methods employed for security protection of communication of data have been developed such as data encrypting and electronic watermark. However, any truly effective method of preventing the image data falsification has not been realized yet.

[0009]

The present invention is made taking the above-described conventional problems into consideration and it is a problem to provide a method of preventing falsification of a photographed image, which is capable of effectively preventing image falsification by authenticating a status that there is no falsification in the image without requiring a recording medium having a specific function.

[0010]

[Means to Solve the Problems]

In order to solve the problem described above, the first aspect of the present invention provides a method of preventing falsification of a photographed image, comprising the steps of: extracting an image characteristic amount by a

specified algorithm from the photographed image in a camera; recording identification information of the photographed image in the camera and said image characteristic amount into a database of an authentication institution which authenticates a status that there is no falsification in the photographed image; extracting an image characteristic amount by said specified algorithm from an authentication object image whose authentication is requested in said authentication institution, and comparing said extracted image characteristic amount with the image characteristic amount recorded in said database, upon the authentication object image in said authentication institution; and judging whether or not said authentication object image is falsified after being photographed, based on consistency between both the image characteristic amounts acquired from said comparison in order to prevent the falsification of the photographed image based on the judgment.

[0011]

Furthermore, in order to solve the problem described above, the second aspect of the present invention provides a method of preventing falsification of a photographed image, comprising the steps of: sending authentication data from an

authentication institution for authenticating a status that there is no falsification in the photographed image to a camera, as well as recording said authentication data and identification information of the photographed image of said camera into a database in said authentication institution; attaching said authentication data to said photographed image or embedding said authentication data into said photographed image with said camera when photographing said photographed image; extracting said authentication data from an authentication object image whose authentication has been requested in said authentication institution, and comparing said extracted authentication data with the authentication data recorded in said database, upon the authentication object image in said authentication institution; and judging whether or not said authentication object image is falsified after being photographed, based on consistency between both the extracted authentication data acquired from said comparison in order to prevent the falsification of the photographed image based on the judgment.

[0012]

[Embodiment of the Invention]

Methods of preventing falsification of a photographed image according to the present invention based on preferred embodiments shown in the accompanied drawings, will be described as follows.

[0013]

Initially, a first embodiment of the present invention is described. In this embodiment, predetermined image characteristic amount data extracted from a photographed image in a camera is sent to an authentication institution, and this authentication institution authenticates the image using the image characteristic amount data.

Fig. 1 is a block diagram schematically showing an embodiment of a system for implementing a method of preventing falsification of photographed image according to a first embodiment of the present invention.

[0014]

In Fig. 1, an authentication institution 10 functions to authenticate a status that a photographed image is photographed by a proper camera 20 registered in the authentication institution 10 and a status that the image is an authentic image which was not falsified after being photographed. The camera (digital still camera) 20 is

registered in the authentication institution 10 in advance. When photographing a subject 30, the camera 20 communicates with the authentication institution 10 and sends information necessary for authenticating the photographed image to the section 10. Then, the camera 20 receives confirmation of registration from the authentication institution 10, and then records the photographed image in a recording medium 40 such as a smart media.

Further, the authentication institution 10 has a database 12 for recording information necessary for authenticating the photographed image, such as identification information of the photographed image and the image characteristic amount which are sent from the camera 20 to the section 10.

[0015]

The photographing method using a camera and the authentication method of authenticating an image according to the embodiment are shown in the flow charts of Figs. 2 and 3 respectively. Operation of this embodiment will be described along with these flow charts.

Note that, in this embodiment, the data is all encrypted and then transmitted in order to prevent a third

person or party from transmitting a counterfeit image while pretending his camera to be the camera 20 registered in the authentication institution 10.

[0016]

At first, description will be made for the photographing method using the camera along with the flow chart shown in Fig. 2. At step 100, the camera 20 is registered in the authentication institution 10 in advance. An ID unique to the camera and key data for encrypting are beforehand assigned to the camera 20 upon shipping or selling of the camera 20. The ID information uniquely identified to the camera is registered in the authentication institution 10. Therefore, registration of the camera is required only once at the beginning.

[0017]

Then, when photographing an image using the camera 20, first at step 110, the authentication institution 10 confirms /authenticates a status that the camera to be used for photographing is the one registered in the authentication institution 10. For this purpose, the camera 20 sends a data registration request signal (information necessary for confirming a status that the camera has been

registered in the authentication institution) to the authentication institution 10. Specifically, the camera 20 encrypts the camera ID information or the like and sends it to the authentication institution 10. Upon receiving the encrypted data registration request signal from the camera 20, the authentication institution 10 decrypts the signal to confirm a status that the camera 20 has already been registered.

The method of confirming registration of the camera 20 using the encryption is not particularly limited, and any well known encrypting technology can be adopted. For example, an example of an authentication method using the encryption is disclosed in the Interface Magazine of February 2000, pp.148 to pp.149.

[0018]

Once the authentication institution 10 confirms a status that the camera 20 has already been registered in the authentication institution 10, the camera 20 photographs the subject 30 at the following step 120.

After photographing, at step 130, the camera 20 creates image characteristic amount data from the photographed image data using a specified algorithm for the authentication

institution 10 to use when authenticating validity of the image later on.

[0019]

Further, a specific algorithm used in creating the image characteristic amount data is not particularly limited. For example, an algorithm can be mentioned, in which an image is divided into some areas (blocks), each having a predetermined size, and edges and spatial frequencies or a histogram of each block are calculated. This algorithm may take in a hardware as a characteristic amount data preparing unit and embedded into the camera 20 after being combined with a photographing device to form a single chip. Thereby, it becomes possible to prevent an interruption of a counterfeit image during the communication.

In addition, this algorithm should be desirably confidential. Further, on the assumption that there may be a case where the algorithm could be decrypted, a plurality of kinds of the algorithm may be prepared, and one of them may be selected randomly in the camera 20 in each photographing session. Alternatively, the algorithm may be selected according to an instruction signal from the authentication institution 10.

[0020]

When the camera 20 selects the algorithm, selection information showing the selection result of the algorithm is added to the image characteristic amount data and sent to the authentication institution 10. Further, when the algorithm is selected according to the instruction signal from the authentication institution 10, the authentication institution 10 is set so as not to receive the signal from the camera 20 during a specified period of time after sending the instruction signal to the camera 20. Thereby, it becomes possible to prevent an interruptive transmission of the already created counterfeit image even if the user of the camera 20 bears harmful intention.

[0021]

Next, at step 140, the camera 20 encrypts the image characteristic amount data just created and photographed image identification information respectively to send them as a set to the authentication institution 10. In this case, the photographed image identification information includes a file name, a camera ID and the like. After the camera is authenticated, the data is transmitted using a common key (secret key) system because the common key system requires

less computing. For example, secret key data unique to each camera is transmitted using a public key system at first, and the secret key data is used for encrypting the image characteristic amount data. Alternatively, other well known encrypting method is used.

Also, as above-mentioned, when the camera 20 selects an algorithm for creating the image characteristic amount data, an algorithm selection information is added to the image characteristic amount data and sent to the authentication institution 10.

The authentication institution 10 records the received image characteristic amount data and the photographed image identification information in the database 12. Then, a kind of the algorithm employed in creating the image characteristic amount data is also recorded.

[0022]

At step 150, when the authentication institution 10 decrypts the above-mentioned received signal and confirms a status that the data is from the authenticated camera, the authentication institution 10 returns a reception confirmation signal to the camera 20.

Next, at step 160, when the camera 20 receives the

confirmation signal, the camera 20 records the photographed image in the recording medium 40. Here, the photographed image identification information is embedded into the photographed image as a header.

[0023]

Photographing process using the camera 20 is carried out as above-mentioned. A recipient of the recording medium 40 with the photographed image recorded therein sends the recorded image data and further the image identification information to the authentication institution 10 using a predetermined communication method and requests authentication of validity of the image.

Following will be described for the authentication process, referring to the flow chart shown in Fig. 3.

[0024]

When the recipient of the photographed image requests falsification check of the image to the authentication institution 10, first at step 200, the image data is transmitted to the authentication institution 10.

Next, at step 210, the authentication institution 10, which has received the image data, reads out the image characteristic amount data corresponding to the previously-

recorded image from the database 12, using the photographed image identification information provided to the header of the image data.

[0025]

At step 220, the authentication institution 10 creates image characteristic amount data from the image to be checked (image to be authenticated) using the same algorithm as the image characteristic amount data creating algorithm employed by the camera 20 during previous photographing. As above-mentioned, a kind of the algorithm employed when the image is photographed is also recorded in the database 12. Therefore, it is possible to use the same algorithm by reading out the kind of the algorithm from the database 12.

[0026]

Subsequently, at step 230, the image characteristic amount data created from the image to be checked is compared with the image characteristic amount data read out from the database 12.

Then, consistency between both data is calculated. If the consistency is equal to a predetermined value or greater, at step 240, it is judged that the image to be checked is not falsified after being photographed. Here, the exact

matching between the data is not required and the consistency equal to a predetermined value or larger is regarded to be sufficient. This is because there is a possibility that information deteriorates due to compression process such as JPEG when recorded using a camera, and the image to be checked is not thus necessarily completely consistent with the original image.

[0027]

As above-mentioned, according to this embodiment, it becomes possible to effectively cope with the case where a counterfeit image is disguised as the image photographed by the authenticated camera and to effectively prevent the photographed image from being falsified.

[0028]

A second embodiment of the present invention will be hereinafter described.

Namely, in the second embodiment, identification information is embedded into image data of a photographed image on the camera side, and an authentication institution authenticates an image by using the identification information.

[0029]

A system for implementing the method for this embodiment is schematically shown in Fig.4.

In Fig.4, an authentication institution 50 functions to authenticate a status that a photographed image is photographed by a camera 60 registered in the authentication institution 50 and a status that the image is an authentic image which was not falsified after being photographed. The camera 60 such as a digital still camera is registered in the authentication institution 50 in advance. When photographing a subject 70, the camera 60 communicates with the authentication institution 50, incorporates watermark information (authentication data) sent from the authentication institution 50 into the photographed image, and then records the photographed image having the watermark information embedded therein in a recording medium 80 such as a smart media.

Further, the authentication institution 50 has a database 52 for recording information necessary for authenticating the photographed image, such as photographed image identification information and image characteristic amount which are sent from the camera 60.

[0030]

The photographing method using the camera according to this embodiment is shown in the flow chart of Fig. 5, and an authentication method thereof is shown in the flow chart of Fig. 6. The image authentication method of this embodiment will be described along with these flow charts.

[0031]

First, the photographing method using the camera will be described along with the flow chart shown in Fig. 5. At step 300, the camera 60 is beforehand registered in the authentication institution 50, similarly to the first embodiment.

Next, when photographing by the camera 60, at step 310, the authentication institution 50 confirms/authenticates a status that the camera to be used for photographing is the one that is registered in the authentication institution 50. Therefore, the camera 60 sends a data registration request signal, including a camera ID and the like, to the authentication institution 50. Upon receiving the encrypted data registration request signal from the camera 60, the authentication institution 50 decrypts the signal to confirm a status that the camera 60 has been already registered.

[0032]

At step 320, the authentication institution 50 generates watermark information (authentication data) unique to a photographed image file, and sends it back to the camera 60. Further, the authentication institution 50 records the watermark information with the camera ID, an image file name and a reception date and time, etc. in the database 52.

At step 330, the camera 60 photographs a subject 70. Then, at step 340, the camera 60 decrypts the watermark information sent back from the authentication institution 50 and incorporates the watermark information into the photographed image.

[0033]

This incorporation method is not particularly limited and any well known embedding algorithm can be adopted. However, the employed embedding algorithm should be desirably confidential. Alternatively, a plurality of algorithms may be prepared. The algorithms may be randomly selected in the camera 60, or the algorithms may be switched corresponding to a selection signal included in the sent back information from the authentication institution 50. Then, in the authentication institution 50, information

concerning which algorithm is employed, is also recorded in the database 52. In addition, identification data of the watermark information may be added as header information of the photographed image in the camera 60.

[0034]

Next, at step 350, the camera 60 records the photographed image data with the watermark information embedded in a recording medium 80.

The photographing process using the camera 60 is carried out as above-mentioned. A recipient of the recording medium 80, in which the photographed image is recorded as above-mentioned, sends the recorded image data to the authentication institution 50 using a predetermined communication unit and requests authentication of validity of the image.

The authentication process will be described along with the flow chart shown in Fig. 6.

[0035]

When the recipient of the photographed image requests falsification check of the image to the authentication institution 50, first at step 400, the image data is transmitted to the authentication institution 50.

At step 410, the authentication institution 50, which has received the image data, reads out from the database 52 the watermark information of the image data corresponding to the image to be checked recorded in the database according to the image file name of the image data and watermark information identification data of the header.

[0036]

Further, the authentication institution 50 extracts the watermark information from the image to be checked in step 420, and at step 430, the authentication institution 50 then compares the watermark information extracted from the image to be checked and the watermark information read out from the database 52. If a degree of consistency is equal to a predetermined value or greater as a result of the comparison, the authentication institution 50 judges at step 440 a status that there is no falsification in the checked image.

[0037]

As above-mentioned, according to this embodiment, since the watermark information is embedded in the image data, it becomes impossible to change only the image data without altering the watermark information. Therefore, it is possible to cope with the case where the image is

counterfeited by manipulating the photographed image and to effectively prevent falsification of the photographed image.

[0038]

Furthermore, as another example, there is a method in which multipoint distance measuring data of a camera and image data characteristic amount are transmitted to an authentication institution as a set and recorded in a database when photographing using the camera. Then, authentication process is implemented by using this data. According to this method, e.g. when counterfeit image data is made by photographing a counterfeit image print, a subject of the counterfeit image can be found as two-dimensional one for its distance measuring data. If an authentic image scene is three-dimensional, the counterfeit image data contradicts it. Therefore, it is possible to judge the presence of falsification based on the contradictions between the distance measuring data and the image data upon authenticating.

[0039]

As above-mentioned in detail, according to each embodiment of the present invention, it is possible to check falsification and counterfeit of the image for cases such as

pretending that a counterfeit image is an image photographed using an authenticated camera and intending to deceive the authentication institution by manipulating the photographed image.

Further, instead of the image as they stand, only the image characteristic amount or the like may be registered. Thereby, data capacity of the authentication institution may be reduced. Thus, it becomes possible to achieve judgment of the image falsification and effective prevention of the image falsification.

[0040]

In the foregoing, the methods of preventing falsification of a photographed image have been described in detail. Note that, however, the present invention is not limited to the above-described examples, and it is a matter of course that various modifications and alterations can be made within the scope of the present invention without departing from the gist of the same.

[0041]

[EFFECTS OF THE INVENTION]

According to the present invention as above-mentioned, it is possible to judge presence of the falsification of a

photographed image and to prevent the falsification of the image. Then the present invention can be carried out without requiring a recording medium having a specific function for cases such as pretending that a counterfeit image is an image photographed using an authenticated camera and intending to deceive the authentication institution by manipulating the photographed image.

[BRIEF DESCRIPTION OF THE DRAWINGS]

[FIG. 1] This is a block diagram schematically showing a system for implementing a method of preventing falsification of photographed image according to a first embodiment of the present invention.

[FIG. 2] This is a flow chart showing a method of photographing using a camera in the first embodiment.

[FIG. 3] This is a flow chart showing a method employed for authentication process also in the first embodiment.

[FIG. 4] This is a block diagram schematically showing a system for implementing a method according to a second embodiment of the present invention.

[FIG. 5] This is a flow chart showing a method of photographing using a camera in the second embodiment.

[FIG. 6] This is a flow chart showing a method employed for

authentication process also in the second embodiment.

[LEGEND]

10, 50 authentication institution

12, 52 database

20, 60 camera

30, 70 subject

40, 80 recording medium

[TYPE OF THE DOCUMENT] Abstract

[ABSTRACT]

[Object] A status in which there is no falsification in an image is authenticated without requiring a recording medium having a specific function.

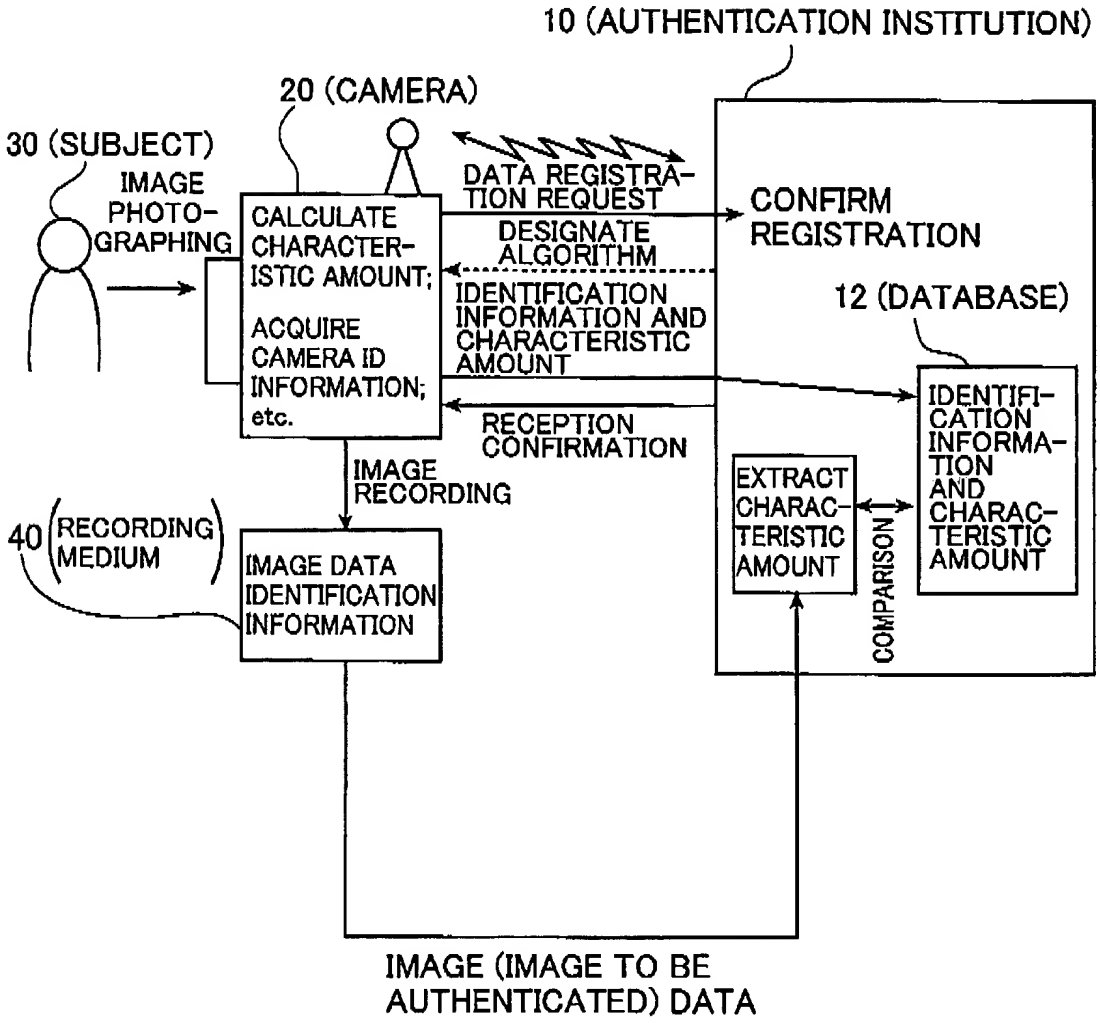
[Means for Solution] The above object can be solved by extracting an image characteristic amount by a specified algorithm from the photographed image in a camera; recording identification information of the photographed image in the camera and the image characteristic amount into a database of an authentication institution which authenticates a status that there is no falsification in the photographed image; extracting an image characteristic amount by the specified algorithm from an authentication object image whose authentication is requested in the authentication institution, and comparing the extracted image characteristic amount with the image characteristic amount recorded in the database, upon the authentication object image in the authentication institution; and judging whether or not the authentication object image is falsified after being photographed, based on consistency between both the image characteristic amounts acquired from the comparison.

[Selected Drawing] FIG. 1

Certificate No. 2001-308313

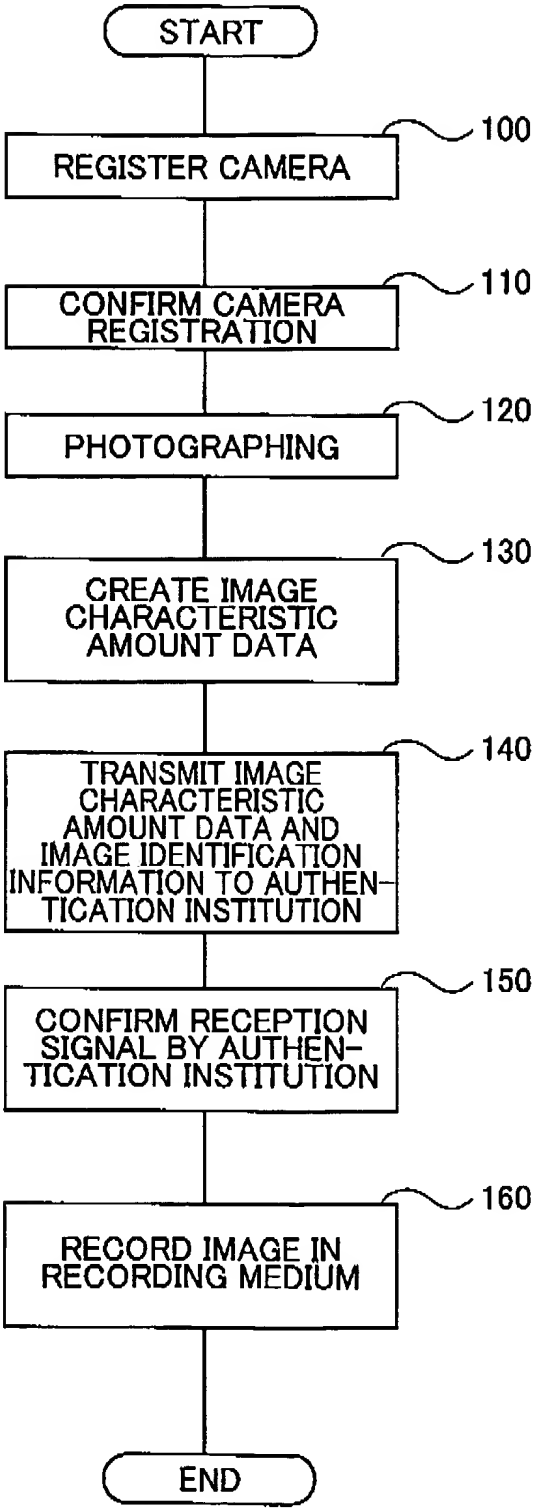
【TYPE OF THE DOCUMENT】 Drawings

【FIG. 1】

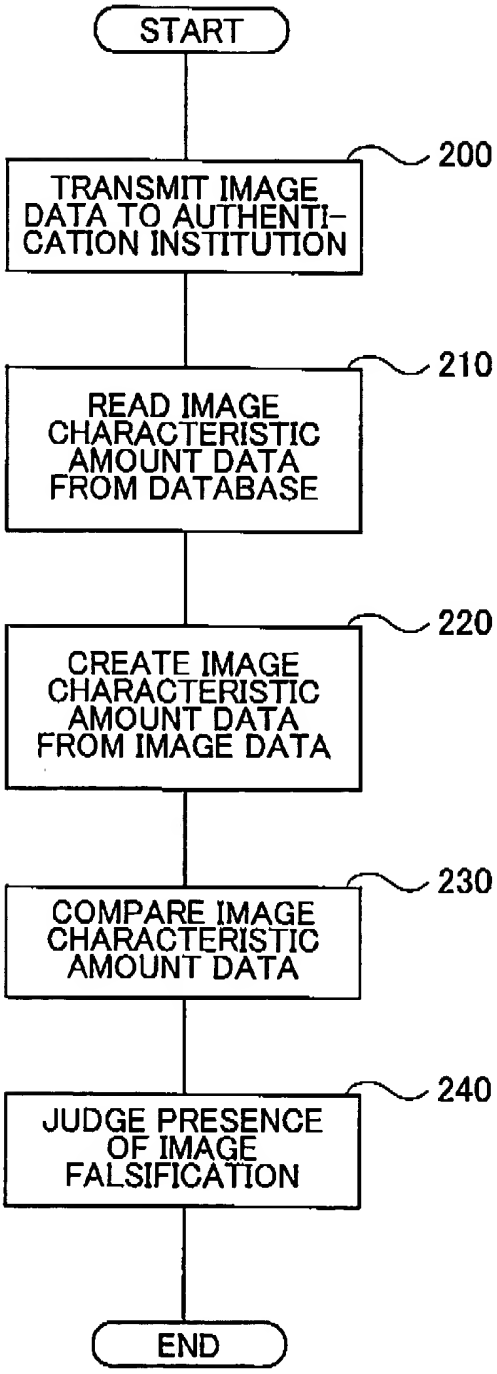


Certificate No. 2001-308313

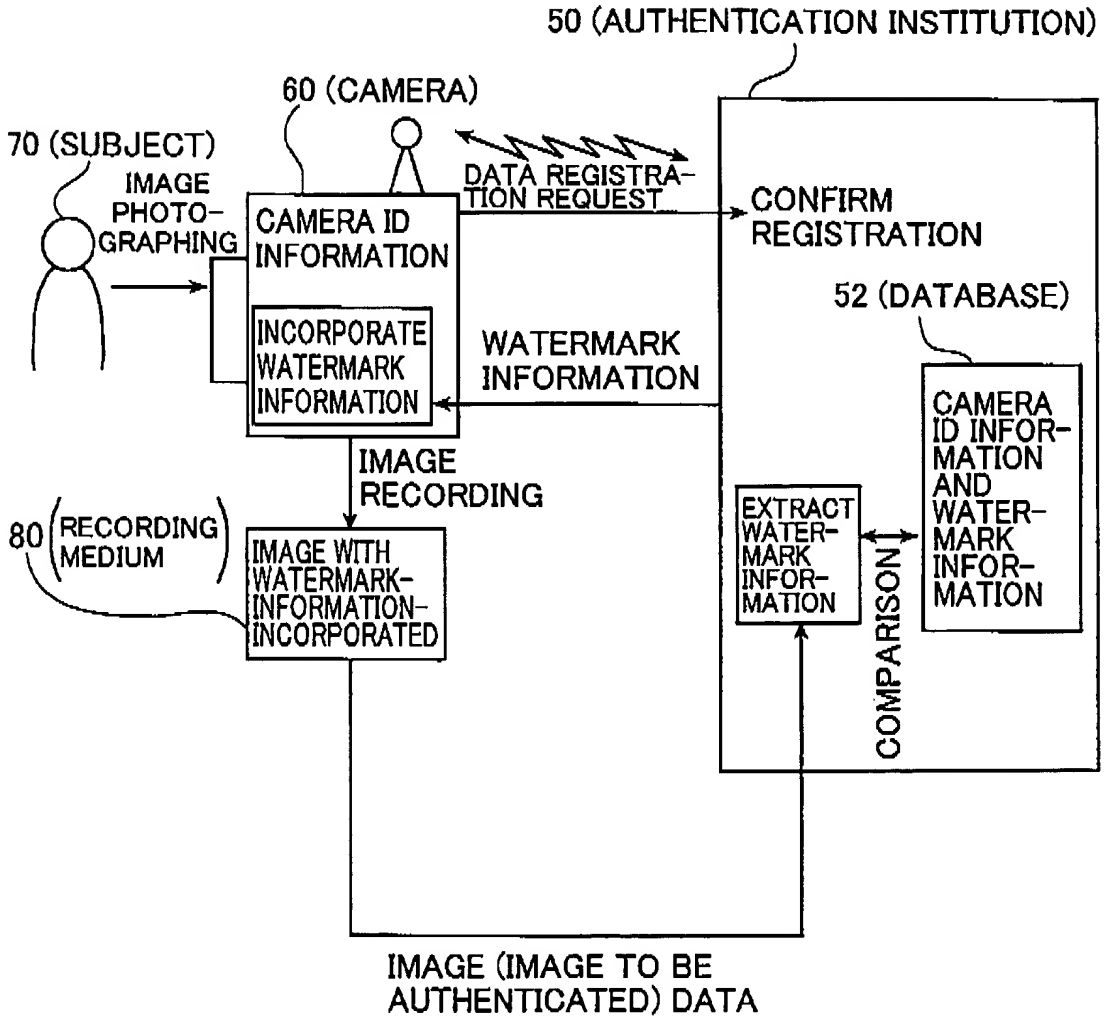
【FIG. 2】



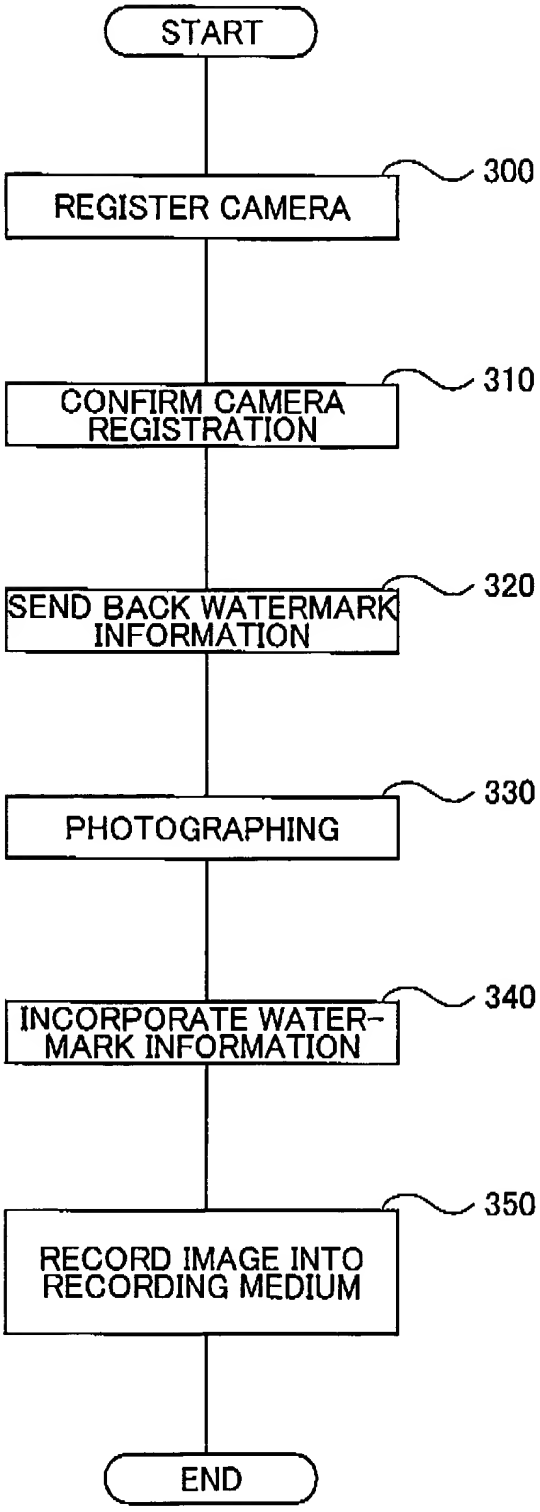
[FIG. 3]



【FIG. 4】

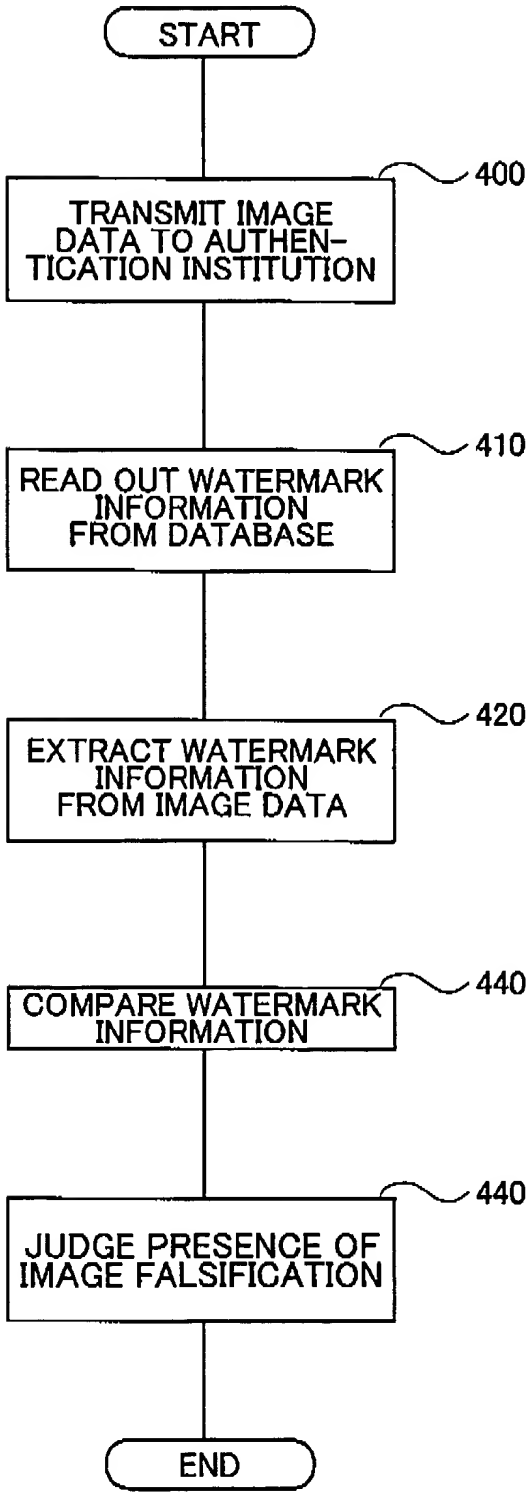


[FIG. 5]



Certificate No. 2001-308313

【FIG. 6】



Certificate No. 2001-308313